H3C SecPath F100-A 防火墙

安装手册

杭州华三通信技术有限公司

http://www.h3c.com.cn

资料版本：T1-08044K-20070419-C-1.03

声明

Copyright ©2006-2007 杭州华三通信技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

H3C、H3C、Aolynk、Aolynk、H^{3}Care、H3care、TOP G、TOPG、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V^{2}G、V^{n}G、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。如需要获取最新手册，请登录http://www.h3c.com.cn。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

前 言

相关手册

手册名称	用途
《H3C SecPath 系列安全产品 操作手册》	介绍 H3C SecPath 系列安全网关/防火墙的功能特性、工作原理和配置及操作指导。
《H3C SecPath 系列安全产品 命令手册》	详细介绍 H3C SecPath 系列安全网关/防火墙所涉及的配置和操作命令。包括命令名、完整命令行、参数、操作视图、使用指导和操作举例。
《H3C SecPath 系列安全产品 Web 配置手册》	指导用户通过 Web 方式对 H3C SecPath 系列防火墙进行配置操作。

本书简介本手册各章节内容如下：

- **第 1 章　产品介绍。**介绍 H3C SecPath F100-A 防火墙的特点及其应用。提供 H3C SecPath F100-A 防火墙的外观图及系统特性描述。
- **第 2 章　安装前的准备工作。**介绍 H3C SecPath F100-A 防火墙对安装环境的要求，以及安装前和安装过程中需要注意的事项，安装所需工具也是本章介绍内容。
- **第 3 章　防火墙的安装。**介绍 H3C SecPath F100-A 防火墙的机械安装方法、电源连接方法，配置口电缆、以太网电缆连接方法。
- **第 4 章　防火墙的启动与配置。**介绍 H3C SecPath F100-A 防火墙的启动与配置基础知识，包括：防火墙的启动、上电、系统文件初始化等内容。
- **第 5 章　防火墙的软件维护。**介绍 H3C SecPath F100-A 防火墙的软件维护，包括：软件升级、配置文件的加载等内容。
- **第 6 章　安装故障处理。**介绍 H3C SecPath F100-A 防火墙安装启动过程中可能出现的问题及检查方法。
- **第 7 章　MIM 多功能接口模块。**介绍 H3C SecPath F100-A 防火墙各功能模块的外观、面板及指示灯的含义，并介绍功能模块的安装及接口电缆的连接方法等。

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | … }	表示从两个或多个选项中选取一个。
[x | y | …]	表示从两个或多个选项中选取一个或者不选。
{ x | y | … }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | …]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入 1～n 次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

⚠ **小心、注意**：提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。

警告：该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。

🕮 **说明、提示、窍门、思考**：对操作内容的描述进行必要的补充和说明。

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

目 录

第 1 章 产品介绍 1-1
1.1 简介 1-1
1.2 硬件特性 1-2
1.2.1 外观 1-2
1.2.2 系统说明 1-3
1.2.3 指示灯含义 1-4
1.2.4 固定接口属性 1-4
第 2 章 安装前的准备工作 2-1
2.1 安装场所要求 2-1
2.1.1 温度/湿度要求 2-1
2.1.2 洁净度要求 2-1
2.1.3 防静电要求 2-2
2.1.4 电磁环境要求 2-2
2.1.5 防雷击要求 2-3
2.1.6 检查安装台 2-3
2.2 安全注意事项 2-3
2.3 检查防火墙及其附件 2-4
2.4 安装工具、仪表和设备 2-4
第 3 章 防火墙的安装 3-1
3.1 安装流程 3-1
3.2 安装到指定位置 3-2
3.2.1 安装到工作台上 3-2
3.2.2 安装到机柜中 3-2
3.3 连接保护地线 3-3
3.4 连接到配置终端 3-4
3.5 连接到以太网口 3-4
3.6 连接电源线 3-5
3.6.1 连接交流电源线 3-6
3.7 安装后的检查 3-6
第 4 章 防火墙的启动与配置 4-1
4.1 启动 4-1
4.1.1 搭建配置环境 4-1
4.1.2 上电 4-3
4.1.3 启动过程 4-4

4.2 配置基础 4-5
4.2.1 基本配置步骤 4-5
4.2.2 命令行接口的特点 4-5
第 5 章 防火墙的软件维护 5-1
5.1 Boot菜单 5-1
5.2 利用XModem协议完成应用程序和Boot ROM程序升级 5-3
5.3 Boot ROM程序扩展段的备份及恢复 5-5
5.4 通过TFTP完成应用程序的升级 5-6
5.5 利用FTP完成程序/文件的上传下载 5-8
5.6 修改Boot ROM口令 5-11
5.7 口令丢失的处理 5-13
第 6 章 安装故障处理 6-1
6.1 电源系统问题故障处理 6-1
6.2 配置系统故障处理 6-1
6.3 应用软件升级故障处理 6-2
第 7 章 MIM多功能接口模块 7-1
7.1 MIM多功能接口模块的种类 7-1
7.2 MIM多功能接口模块的安装与拆卸 7-1
7.3 MIM接口模块的故障处理 7-2
7.4 1FE/2FE/4FE接口模块 7-3
7.4.1 简介 7-3
7.4.2 接口模块外观 7-3
7.4.3 接口属性 7-4
7.4.4 面板及接口指示灯 7-5
7.4.5 接口连接电缆 7-5
7.4.6 接口电缆的连接 7-7
7.5 HNDE模块 7-7
7.5.1 模块简介 7-7
7.5.2 模块属性 7-8
7.5.3 模块运行指示灯 7-8
7.5.4 模块故障排除 7-8

插图目录

图 1-1 H3C SecPath F100-A防火墙前面板示意图 1-2
图 1-2 H3C SecPath F100-A防火墙后面板示意图 1-3
图 3-1 防火墙的安装流程 3-1
图 3-2 防火墙机柜安装示意图 3-3
图 3-3 配置口电缆示意图 3-4
图 3-4 以太网电缆示意图 3-5
图 4-1 通过CONSOLE口进行本地配置示意图 4-1
图 4-2 新建连接 4-1
图 4-3 本地配置连接端口设置 4-2
图 4-4 串口参数设置 4-2
图 4-5 终端类型设置 4-3
图 5-1 [发送文件]对话框 5-4
图 5-2 正在发送文件界面 5-4
图 5-3 搭建FTP本地上传/下载环境 5-8
图 5-4 搭建FTP远程上传/下载环境 5-9
图 7-1 MIM多功能接口模块安装示意图 1 7-2
图 7-2 MIM多功能接口模块安装示意图 2 7-2
图 7-3 1FE接口模块外观 7-3
图 7-4 2FE接口模块外观 7-4
图 7-5 4FE接口模块外观 7-4
图 7-6 1FE接口模块面板 7-5
图 7-7 2FE接口模块面板 7-5
图 7-8 4FE接口模块面板 7-5
图 7-9 以太网电缆 7-5
图 7-10 5 类双绞线示例图 7-6
图 7-11 HNDE模块面板 7-8

表格目录

表 1-1 H3C SecPath F100-A防火墙的系统说明表 1-3
表 1-2 H3C SecPath F100-A防火墙前面板指示灯含义 1-4
表 1-3 配置口属性 1-4
表 1-4 备份口属性 1-4
表 1-5 以太网接口属性 1-5
表 2-1 机房温度/湿度要求 2-1
表 2-2 机房灰尘含量限值 2-1
表 2-3 机房有害气体限值 2-2
表 3-1 H3C SecPath F100-A防火墙外形尺寸 3-2
表 7-1 1FE/2FE/4FE模块接口属性 7-4
表 7-2 1FE/2FE/4FE接口模块指示灯含义 7-5
表 7-3 标准（直通）网线连接关系表 7-6
表 7-4 交叉网线连接关系表 7-6
表 7-5 HNDE模块属性 7-8
表 7-6 HNDE模块指示灯含义 7-8

第1章 产品介绍

1.1 简介

H3C SecPath F100-A 防火墙设备（以下简称防火墙）是面向企业用户开发的新一代专业防火墙设备，可以作为中小企业的出口防火墙设备，也可以作为中型企业的内部防火墙设备。

H3C SecPath F100-A 提供了 3 个固定的 10/100M 自适应 FE 端口（WAN）和 4 个 10/100M 自适应交换以太网口；还提供了一个 MIM 扩展槽位，以支持多种 VPN 接入手段，可选的接口模块有 1FE/2FE/4FE、HNDE。

H3C SecPath F100-A 防火墙采用 ASPF 状态检测技术，可对连接过程和有害命令进行监测，并协同 ACL 完成动态包过滤。

H3C SecPath F100-A 防火墙支持 AAA、NAT 等技术，可以确保在开放的 Internet 上实现安全的、满足可靠质量要求的私有网络。

H3C SecPath F100-A 防火墙支持多种 VPN 业务，如 L2TP VPN、IPsec VPN、GRE VPN、动态 VPN 等，可以针对客户需求通过拨号、租用线、VLAN 或隧道等方式接入远端用户，构建 Internet、Intranet、Access 等多种形式的 VPN。

H3C SecPath F100-A 防火墙提供基本的路由能力，支持 RIP/OSPF 路由策略及策略路由；支持丰富的 QoS 特性，提供流量监管、流量整形及多种队列调度策略。

H3C SecPath F100-A 防火墙设备的主要特点如下：

1. 提供 IP VPN 解决方案

随着网络的发展，可以为企业日常工作带来很多方便。企业总部可以通过网络向企业分支机构发布一些重要信息。通过 Internet 实现企业间的内部互联需要应用 VPN 技术。H3C SecPath F100-A 防火墙提供了丰富的 IP VPN 业务：L2TP/GRE 分别提供二层隧道和三层隧道功能；IPSEC 提供经过安全封装的隧道，为网络提供了更高的安全性。

2. 数据安全性及可靠性

- 为保护网络安全，基于访问控制列表的包过滤可以在网络层和传输层检测数据包，防止非法入侵。ASPF 能够检测应用层协议的信息，并对应用的流量进行监控。包过滤和状态检测防火墙的实现可以防止来自外部网络的入侵。
- 支持 NAT（Network Address Translation）特性。除基本功能外，防火墙的 NAT 特性还支持对单独用户并发连接数目进行限制，在满足通常网络应用的同

时又减少了资源被恶意占用，避免了对网络造成的冲击。此外，还有增强的 NAT ALG 功能，对 H.323、FTP、ICMP 等提供 NAT 穿越功能。

- 支持 AAA、RADIUS 身份验证协议。
- 支持 VPN（包括 GRE、L2TP），提供了 IPsec、IKE 等技术，保障了用户在 Internet 环境下私有网络的安全性。
- 路由协议 OSPF、RIP2 都具有 MD5 认证功能，确保所交换路由信息的可靠性。
- 提供 VRRP（Virtual Router Redundancy Protocol）技术，确保通信线路或设备发生故障时可提供备用方案，有效增强了网络的强壮性和可靠性。

3. 支持在线升级软件版本

软件可以根据需求实现应用程序、Boot ROM 程序的在线升级，增加新特性、扩充新功能。

4. 网络管理功能

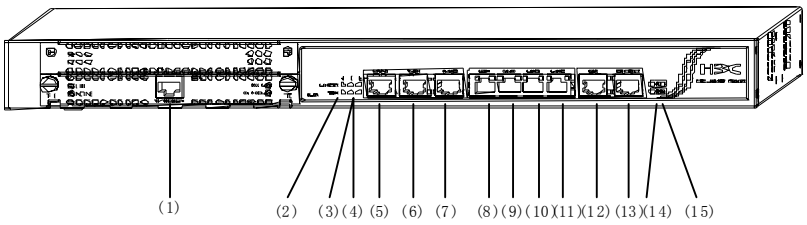
H3C SecPath F100-A 防火墙支持 SNMP V3 网管，并且兼容 SNMP V2C、SNMP V1，为用户提供强大的设备管理功能。

5. 通过的认证

H3C SecPath F100-A 防火墙按照中国、北美、欧洲、澳洲、日本等国家和地区的国际标准和国家标准设计，满足这些国家和地区的 EMC、安规等认证及入网需求。

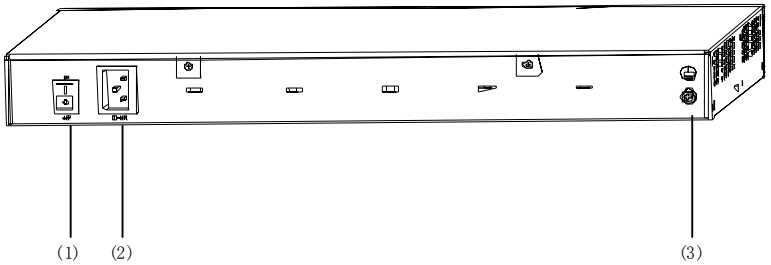
1.2 硬件特性

1.2.1 外观



(1) MIM 接口卡插槽
(2) 固定广域网口 0 的两个指示灯
(3) 固定广域网口 1 的两个指示灯
(4) 固定广域网口 2 的两个指示灯
(5) 固定广域网接口 0（WAN0）
(6) 固定广域网接口 1（WAN1）
(7) 固定广域网接口 2（WAN2）
(8) 固定以太网口 0（LAN0）
(9) 固定以太网口 1（LAN1）
(10) 固定以太网口 2（LAN2）
(11) 固定以太网口 3（LAN3）
(12) 备份口（AUX）
(13) 配置口（CONSOLE）
(14) 系统指示灯（SYS）
(15) 电源指示灯（PWR）

图1-1 H3C SecPath F100-A 防火墙前面板示意图



(1) 电源开关 (2) 电源插座 (3) 接地端子

图1-2 H3C SecPath F100-A 防火墙后面板示意图

1.2.2 系统说明

表1-1 H3C SecPath F100-A 防火墙的系统说明表

项目	防火墙描述
MIM 插槽	1
固定接口	4 个 10/100Mbps LAN 以太网交换口，3 个 10/100Mbps WAN 以太网口 1 个 AUX 口(备份口) 1 个 CONSOLE 口(配置口)
Boot ROM	512KB
DDR SDRAM	256MB
Flash	16MB
外型尺寸（W×D×H）	436 mm×330 mm×44 mm（不含脚垫）
重量	4kg
电源输入	额定电压范围：100～240V AC；50/60Hz 额定电流：1.5A
最大功率	54W
工作环境温度	0～40℃
环境相对湿度	10%～90%（非凝露）

📖 **说明：**

DDR SDRAM（双倍数据速率同步动态随机存取存储器）是常说的内存，存储系统运行时的程序和与 CPU 的通信数据。

1.2.3 指示灯含义

表1-2 H3C SecPath F100-A 防火墙前面板指示灯含义

指示灯	含义
PWR	系统电源指示灯，灯灭表示电源没有接通，灯亮表示电源已接通。
SYS	硬件系统运行指示灯，灯闪烁表示系统正常运行，灯灭表示系统工作不正常。
LINK/ACT	灯灭表示链路没有连通，灯亮表示链路已经连通；灯闪烁表示有数据收发。
100M	灯灭表示该接口工作在 10Mbps 的数据收发速度下，灯亮表示该接口工作在 100Mbps 的数据收发速度下。

1.2.4 固定接口属性

1. 配置口(CONSOLE)

表1-3 配置口属性

属性	描述
连接器类型	RJ45
接口标准	RS232
波特率	1200bps～115200bps 缺省 9600bps
支持服务	与字符终端相连 与本地 PC 的串口相连，并在 PC 上运行终端仿真程序 命令行接口

2. 备份口(AUX)

表1-4 备份口属性

属性	描述
连接器类型	RJ45
接口标准	RS232
波特率	1200bps~115200bps
支持服务	Modem 拨号 备份

3. 以太网口

H3C SecPath F100-A 为用户提供了七个 10/100Mbps 自适应快速以太网接口，其接口特性如下：

表1-5 以太网接口属性

属性	描述
连接器类型	RJ45
接口类型	LAN 口和 WAN 口均支持 MDI/MDIX 自适应
支持帧格式	Ethernet_II Ethernet_SNAP
工作方式	10/100Mbps 自适应 全双工/半双工

第2章 安装前的准备工作

2.1 安装场所要求

H3C SecPath F100-A 防火墙必须在室内使用，为保证防火墙正常工作和延长使用寿命，安装场所应该满足下列要求。

2.1.1 温度/湿度要求

为保证防火墙正常工作，并延长使用寿命，机房内需维持一定的温度和湿度。若机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，还会发生材料机械性能变化、金属部件锈蚀等现象；若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，在干燥的气候环境下，还容易产生静电，危害防火墙上的 CMOS 电路；温度过高危害更大，因为高温会加速绝缘材料的老化过程，使防火墙的可靠性大大降低，严重影响其使用寿命。

H3C SecPath F100-A 防火墙对温度、湿度的要求见下表。

表2-1 机房温度/湿度要求

温度	相对湿度
0℃～40℃	10%～90%（非凝露）

2.1.2 洁净度要求

灰尘对防火墙的运行安全也是一大危害，因为室内灰尘落在机体上会造成静电吸附，使金属接插件或金属接点接触不良，不但会影响设备寿命，而且容易造成通信故障。当室内相对湿度偏低时，更易产生这种静电吸附。

防火墙对机房的要求为机房无爆炸性、导电性、导磁性及腐蚀性尘埃，灰尘浓度符合下表的要求：

表2-2 机房灰尘含量限值

机械活性物质	单位	含量
灰尘粒子	粒/m³	≤3×10^4 （3 天内桌面无可见灰尘）
注：灰尘粒子：直径≥5μm		

除灰尘外，H3C SecPath F100-A防火墙的机房对空气中所含的盐、酸、硫化物也有严格的要求，因为这些有害气体会加速金属的腐蚀和某些部件的老化过程。机房内对SO_2、H_2S、NH_3、Cl_2等有害气体的具体限制值见下表：

表2-3 机房有害气体限值

气体	最大（mg/m3）
二氧化硫SO_2	0.2
硫化氢H_2S	0.006
氨NH_3	0.05
氯气Cl_2	0.01

2.1.3 防静电要求

尽管 H3C SecPath F100-A 防火墙在防静电方面作了大量的考虑，采取了多种措施，但当静电超过一定限度时，仍会对单板电路乃至防火墙整机产生巨大的破坏作用。

在与防火墙连接的通信网中，静电感应主要来自两个方面：一是室外高压输电线、雷电等外界电场；二是室内环境、地板材料、整机结构等内部系统。因此为防止静电损伤，应做到：

- 设备良好接地。
- 室内防尘。
- 保持适当的温度、湿度条件。
- 接触电路板时，应戴防静电手腕，穿防静电工作服。
- 将拆卸下的电路板面朝上放置在抗静电的工作台上或放入防静电袋中。
- 当观察或转移拆卸了的电路板时，请用手接触电路板的外边缘，避免用手直接触摸电路板上的元器件。

2.1.4 电磁环境要求

防火墙使用中可能的干扰源，无论是来自设备或应用系统外部，还是来自内部，都是以电容耦合、电感耦合、电磁波辐射、公共阻抗（包括接地系统）耦合的传导方式对设备产生影响，因此为达到抗干扰的要求，应做到：

- 对供电系统采取有效的防电网干扰措施。
- 防火墙工作地最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能相距远一些。
- 远离强功率无线电发射台、雷达发射台、高频大电流设备。
- 必要时采取电磁屏蔽的方法。

2.1.5 防雷击要求

尽管 H3C SecPath F100-A 防火墙在防雷击方面作了大量的考虑，也采取了必要措施，但是在雷击强度超过一定范围时，仍然有可能对防火墙造成损害。为达到更好的防雷效果，建议用户：

- 保证机箱的保护地用保护地线与大地保持良好接触。
- 保证电源插座的接地点与大地良好接触。
- 为增强电源的防雷击效果，可以考虑在电源的输入前端加入电源避雷器，这样可大大增强电源的抗雷击能力。

2.1.6 检查安装台

对 H3C SecPath F100-A 防火墙进行安装前要保证以下条件：

- 确认防火墙的入风口及通风口处留有空间，以利于防火墙机箱的散热。
- 确认机柜自身有良好的通风散热系统。
- 确认机柜足够牢固，能够支撑防火墙及其安装附件的重量。
- 确认机柜良好接地。

2.2 安全注意事项

基于防火墙的广泛应用及其在数据通信网络中担当的重要作用，再次强调手册中的如下标志，阅读过程中请注意：

警告：表明该项操作不正确，可能给防火墙或防火墙操作者的人身安全带来极大危险，操作者必须严格遵守正确的操作规程。

注意：表示在安装、使用防火墙中需要注意的操作。该操作不正确，可能影响防火墙的正常使用。

在防火墙的安装和使用过程中，特提出如下安全建议：

- 请将防火墙放置在远离潮湿或远离热源的地方。
- 请确认防火墙已经正确接地。
- 请在安装维护过程中佩戴防静电手腕，并确保防静电手腕与皮肤良好接触。
- 请不要带电插拔配置口(Console)、备份口(AUX)的电缆。
- 建议用户使用 UPS（Uninterrupted Power Supply，不间断电源）。

2.3 检查防火墙及其附件

在确认安装环境符合要求后，请打开防火墙包装箱，并对照定货合同及装箱单仔细核对防火墙及附件是否齐全。如有疑问或差错，请与代理商联系。

2.4 安装工具、仪表和设备

1. 工具

- 十字螺丝刀
- 防静电手腕
- 防静电袋

2. 电缆

- 地线及电源线
- 配置口（Console）电缆
- 可选电缆

3. 设备及仪表

- HUB 或 LAN Switch
- 配置终端（可以是普通的 PC 机）
- 万用表

🕮 **说明：**

防火墙不附带安装工具、仪表及相关设备。

第3章 防火墙的安装

3.1 安装流程

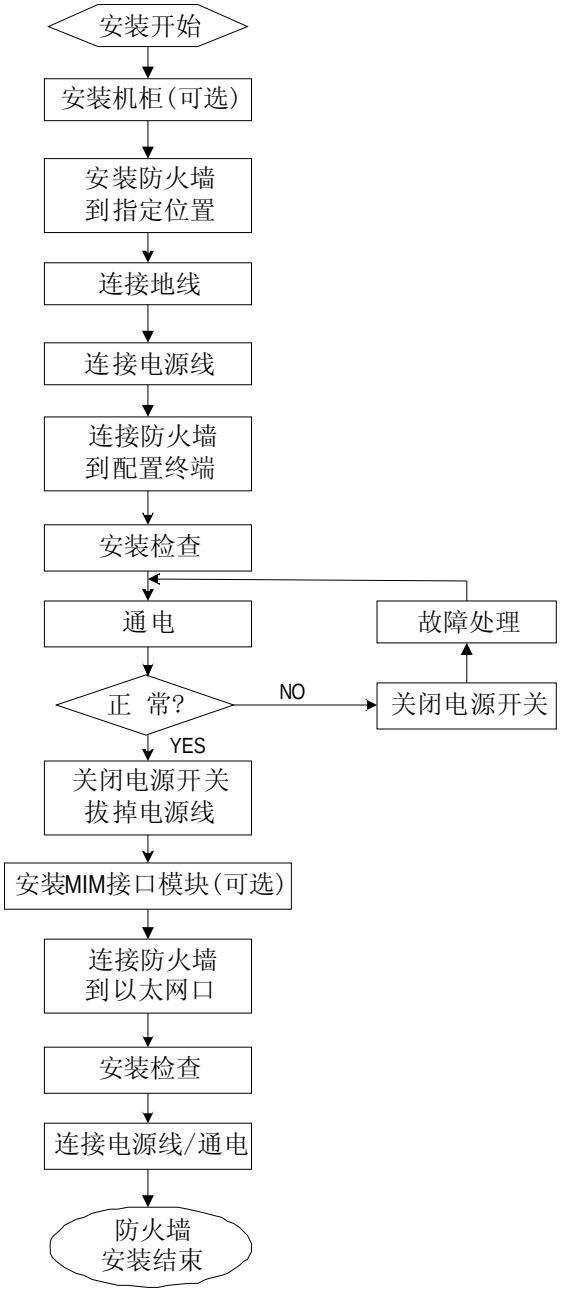


图3-1 防火墙的安装流程

⚠ 注意：

开始安装 H3C SecPath F100-A 防火墙前，请确认：

- 已经仔细阅读第二章内容。
- 第二章中所述要求已经满足。

3.2 安装到指定位置

H3C SecPath F100-A 防火墙有两种安装方式:

- 直接安放在平台上
- 安装到机柜上

3.2.1 安装到工作台上

多数情况下，用户并不具备 19 英寸标准机柜，人们更常用到的方法就是将防火墙放置在干净的工作台上。此种操作比较简单，操作中需要注意如下事项：

- 保证工作台的平稳性与良好接地。
- 防火墙四周留出 10cm 的散热空间。
- 不要在防火墙上面放置重物。

3.2.2 安装到机柜中

H3C SecPath F100-A 防火墙是按照 19 英寸标准机柜的尺寸进行设计的，尺寸如下表：

表3-1 H3C SecPath F100-A 防火墙外形尺寸

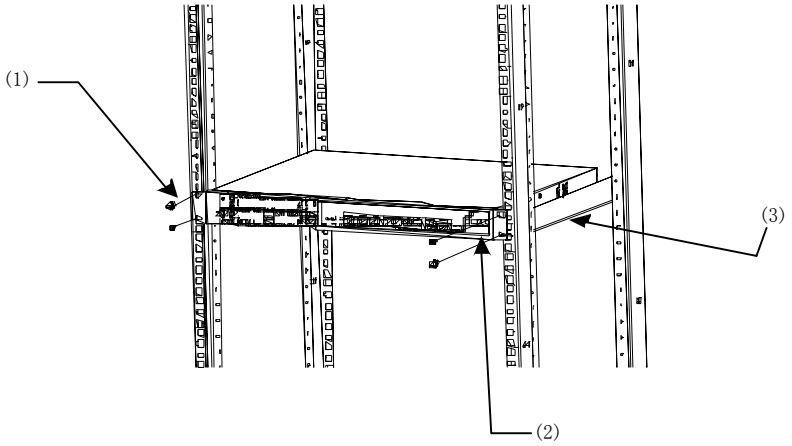
防火墙型号	外形尺寸（单位：mm）
H3C SecPath F100-A 防火墙（W×D×H）	436×330×44（不含脚垫）

H3C SecPath F100-A 防火墙安装过程如下：

第一步：检查机柜的接地与稳定性。用螺钉将固定挂耳固定在防火墙前面板两侧；

第二步：将防火墙放置在机柜的一个托盘上，根据实际情况，沿机柜导轨移动防火墙至合适位置，注意保证防火墙与导轨间的合适距离；

第三步：用满足机柜安装尺寸要求的盘头螺钉（螺钉型号最大不得超过国标 M6，表面经过防锈处理）将防火墙通过固定挂耳固定在机柜上，保证防火墙在机柜上位置水平并牢固。



(1) 固定螺钉（4 个） (2) 固定挂耳 (3) 导轨

图3-2 防火墙机柜安装示意图

3.3 连接保护地线

警告：

防火墙保护地线的正常连接是防火墙防雷、抗干扰的重要保障，所以用户在安装、使用防火墙时必须首先正确接好保护地线。

H3C SecPath F100-A 防火墙提供单独的保护地端子，保护地必须良好接地，以使感应电、泄漏电能够安全流入大地，并提高整机的抗电磁干扰的能力。

H3C SecPath F100-A防火墙的保护地端子位于机箱后面板的右下侧，有接地标识，见图 1-2。

请用一根保护地电缆（PGND Cable）将该点与大地连接起来，要求接地电阻不大于 5Ω。如果防火墙是安装在 19 英寸标准机柜上，则同样要求 19 英寸标准机柜接地。

警告：

防火墙正常工作时必须良好接地（保护地），否则防火墙无法可靠防雷，从而有可能造成防火墙及对端设备的损坏！

3.4 连接到配置终端

1. 配置口介绍

H3C SecPath F100-A防火墙提供了一个RS232 异步串行配置口（CONSOLE），通过这个接口用户可完成对防火墙的配置。配置口的属性请参见1.2.4 固定接口属性一节。

2. 配置口电缆

配置口电缆是一根 8 芯屏蔽电缆，一端压接 RJ45 插头，插入防火墙的 CONSOLE 口；另一端则带有一个 DB9（母）连接器，可插入配置终端的串口。

配置口电缆如图 3-3所示：

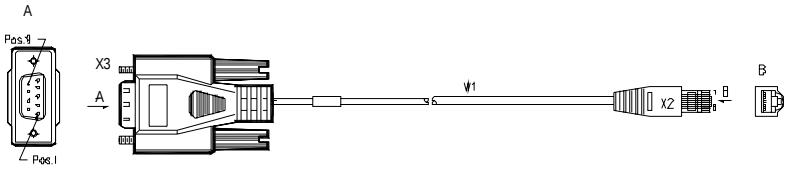


图3-3 配置口电缆示意图

3. 连接配置口电缆

通过终端配置防火墙时，配置口电缆的连接步骤如下：

第一步：选定配置终端。配置终端可以是标准的具有 RS232 串口的字符终端，也可以是一台普通的 PC 机，更常用的是后者。

第二步：连接电缆。关闭防火墙、配置终端的电源，通过配置电缆将配置终端的 RS232 串口与防火墙上的配置口相连。

经安装检查后加电，正常情况下将在配置终端上显示防火墙启动信息，详细内容请参见《第 4 章 防火墙的启动与配置》。

3.5 连接到以太网口

1. 以太网接口介绍

H3C SecPath F100-A 防火墙提供了四个固定的快速以太网口做为下行通道，可进行 10/100Mbps 自适应。H3C SecPath F100-A 防火墙还提供了三个固定的快速以太网口做为上行通道，可进行 10/100Mbps 自适应，通过以太网接入到路由器、交换机等设备。

📖 说明：

H3C SecPath F100-A 防火墙的四个 LAN 以太网接口既可以工作在三层模式下，也可以工作在 Hub 方式下。当在系统视图下执行 **insulate** 命令时，四个 LAN 以太网接口都将工作在三层模式下，这时防火墙的 LAN0、LAN1、LAN2 和 LAN3 接口分别对应命令行中的 E0/0、E0/1、E0/2 和 E0/3 接口；当在系统视图下执行 **undo insulate** 命令时，四个 LAN 以太网接口都将工作在 Hub 方式下，这时防火墙的 LAN0、LAN1、LAN2 和 LAN3 接口则只对应命令行中的一个 E0/0 接口；WAN0、WAN1 和 WAN2 接口分别对应命令行中的 E1/0、E1/1 和 E1/2 接口。

2. 以太网线缆

H3C SecPath F100-A防火墙以太网接口采用 5 类双绞线连接以太网，电缆外观如图 3-4所示：

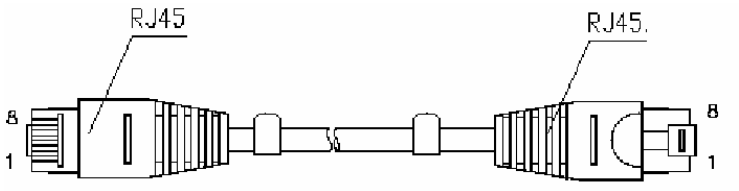


图3-4 以太网电缆示意图

📖 说明：

用户制作网线时，请优先采用屏蔽电缆，以保证电磁兼容的需要。

3. 连接以太网线缆

以连接 H3C SecPath F100-A 防火墙正面板上的固定 LAN0 接口为例，请按照下述步骤连接：

⚠ 注意：

连接时请认准接口上的标识，以免误插入其它接口。

第一步：将以太网电缆一端连接到防火墙，另一端连接到对端设备；

第二步：请检查 LAN0 接口 LINK 指示灯的状态，LINK/ACT 灯亮表示以太网口链路已经连通，LINK 灯灭表示以太网口链路没有连通，请检查线路。

3.6 连接电源线

H3C SecPath F100-A 防火墙提供交流供电机型。

3.6.1 连接交流电源线

1. 交流电源

交流电源输入范围：100～240V AC；50/60Hz。

交流供电防火墙的电源插座部分外观如图 1-2所示：

2. 建议使用的交流电源插座

建议使用有接地点接头的单相三线电源插座。电源的接地点在建筑物中要可靠接地，一般楼房在施工布线时，已将本楼供电系统的电源接地点埋地。连接防火墙交流电源线前，用户需要确认本楼电源是否已经接地。

3. 交流电源线的连接

第一步：确认保护地已经正确连接至大地。

第二步：确认防火墙供电电源开关置于 OFF 位置后，将防火墙随机所带的电源线一端插到防火墙机箱后面板左侧的 100-240V AC 电源插座上，另一端插到交流供电电源插座上。

第三步：把防火墙供电电源开关拨到 ON 位置。

第四步：把防火墙 PWR 电源开关拨到 ON 位置。

第五步：检查防火墙前面板电源灯 PWR 是否变亮，灯亮则表示电源连接正确。

第六步：检查防火墙前面板硬件系统指示灯 SYS 是否闪烁，灯闪烁表明硬件系统正常。

3.7 安装后的检查

在 H3C SecPath F100-A 防火墙安装过程中，两次加电前均要进行安装检查，检查事项如下：

- 请检查防火墙周围是否留有足够的散热空间，机柜是否稳固。
- 检查电源线所接电源与防火墙要求的电源是否一致。
- 检查防火墙的保护地线是否连接正确。
- 检查防火墙与配置终端等其它设备的连接关系是否正确。

📖 **说明：**

防火墙安装完毕后的检查非常重要，因为防火墙安装的牢固与否、接地良好与否、电源匹配与否，将直接关系到防火墙的正常使用。

第4章 防火墙的启动与配置

4.1 启动

第一次安装使用 H3C SecPath F100-A 防火墙时，只能通过配置口（Console）进行配置。

4.1.1 搭建配置环境

1. 连接防火墙到配置终端

如图 4-1 所示，将配置口电缆的 RJ45 一端与防火墙的配置口相连，DB9 一端与微机的串口相连。

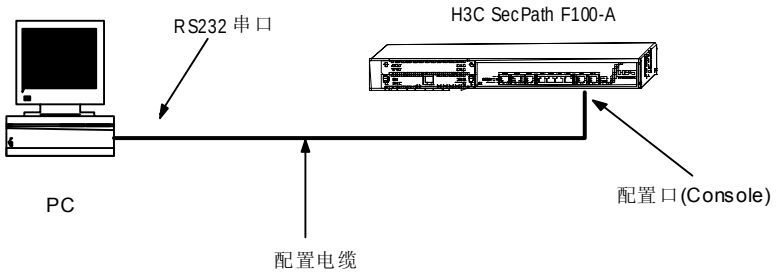


图4-1 通过 CONSOLE 口进行本地配置示意图

2. 设置配置终端的参数

第一步：打开配置终端，建立新的连接。

如果使用微机进行配置，需要在微机上运行终端仿真程序（如 Windows3.1 的 Terminal，Windows95/Windows98/Windows NT 的超级终端），建立新的连接。如图 4-2 所示，键入新连接的名称，按［确定］按钮。

图4-2 新建连接

第二步：设置终端参数。

Windows98 超级终端参数设置方法如下：

(1) 选择连接端口

在进行本地配置时，如图 4-3 所示，［连接时使用］一栏选择连接的串口（注意选择的串口应该与配置电缆实际连接的串口一致）。

图4-3 本地配置连接端口设置

(2) 设置串口参数

如图 4-4 所示，在串口的属性对话框中设置波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无，按［确定］按钮，返回超级终端窗口。

图4-4 串口参数设置

(3) 配置超级终端属性

在超级终端中选择［属性/设置］一项，进入图 4-5 所示的属性设置窗口。选择终端仿真类型为 VT100 或自动检测，按［确定］按钮，返回超级终端窗口。

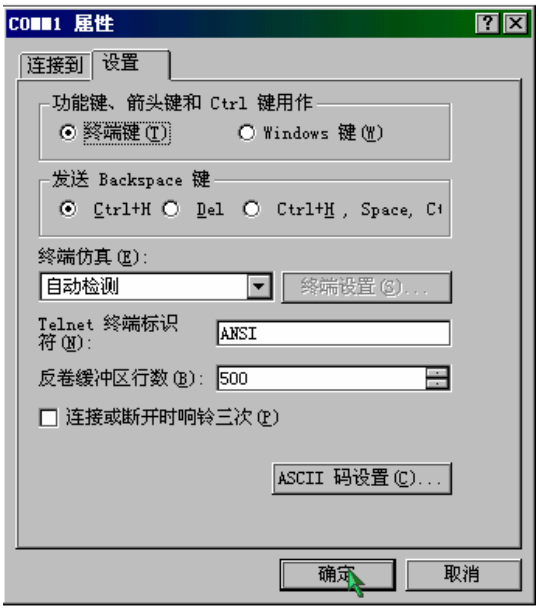


图4-5 终端类型设置

4.1.2 上电

1. 上电前检查

防火墙上电之前应进行如下检查：

- 电源线和地线连接是否正确。
- 供电电压与防火墙的要求是否一致。
- 配置电缆连接是否正确，配置用微机或终端是否已经打开，并设置完毕。

警告：

上电之前，要确认设备供电电源开关的位置，以便在发生事故时，能够及时切断供电电源。

2. 上电

- 打开防火墙供电电源开关。
- 打开防火墙电源开关（将防火墙电源开关置于 ON 位置）。

3. 上电后检查/操作

防火墙上电后，要进行如下检查：

- 防火墙前面板上的指示灯显示是否正常。

检查方法：防火墙上电后，正常运行过程中各指示灯状态请参见1.2.3 中关于指示灯含义的描述。

- 配置终端是否显示正常。

检查方法：防火墙上电后，可在配置终端上直接看到启动界面（参见4.1.3 ）。启动结束后将提示用户键入回车，当出现命令行提示符“<H3C>”时即可进行配置了。

4.1.3 启动过程

防火墙上电开机后，将首先运行 Boot ROM 程序，终端屏幕上显示如下系统信息：

📖 **说明：**

对于不同版本的 Boot ROM，终端上显示的界面可能会略有差别。

```
**************************************************
*                                                *
*  H3C SecPath Series Gateway Boot ROM V1.17     *
*                                                *
**************************************************

Copyright(C) 2004-2007 by Hangzhou H3C Technologies Co.,Ltd.
Compiled at Wed Apr 12 17:39:36 CST 2006

 Testing memory...OK!
 256M bytes DDR SDRAM Memory
 16M  bytes Flash Memory
 Hardware Version is 3.0
 CPLD     Version is 1.0

Press Ctrl-B to enter Boot Menu
```

若此时按下<Ctrl+B>键，系统将进入 Boot 菜单；否则，系统将进入程序解压过程。

📖 **说明：**

必须在出现“Press Ctrl-B to Enter Boot Menu...”的 3 秒钟之内，按下<Ctrl+B>键，才能进入 Boot 菜单。

系统解压缩、初始化屏幕显示如下：

```
System is self-decompressing.....................................

System is starting...

User interface Con 0 is available.
```

```
Press ENTER to get started.
```

键入<Enter>屏幕出现（若没有设置登录验证）：

```
<H3C>
```

该提示符表明防火墙已经进入用户视图，可以对防火墙进行配置了。

4.2 配置基础

4.2.1 基本配置步骤

一般情况下配置防火墙的基本思路如下：

第一步：在配置防火墙之前，需要将组网需求具体化、详细化，包括：组网目的、防火墙在网络互连中的角色、传输介质的选择、网络的安全策略和网络可靠性需求等；

第二步：然后根据以上要素绘出一个清晰完整的组网图；

第三步：配置防火墙各接口的 IP 地址；

第四步：配置路由，如果需要启动动态路由协议，还需配置相关动态路由协议的工作参数；

第五步：如果有特殊的安全需求，则需进行防火墙的安全性配置；

第六步：如果有特殊的可靠性需求，则需进行防火墙的可靠性配置。

关于防火墙各协议或功能配置的详细介绍，请参见相应产品的操作手册和命令手册。

4.2.2 命令行接口的特点

1. 命令行接口的特点

防火墙向用户提供的命令行接口包括一系列的配置命令，用户可以通过这些命令来配置和管理防火墙，命令行接口有如下的特点：

- 通过 CONSOLE 口进行本地配置；
- 通过 Telnet 进行本地或远程配置，可以用 Telnet 命令直接登录并管理其它通信设备；
- 用户可以随时键入“？”而获得在线帮助；
- 提供全中文的提示和帮助信息，方便国内广大用户；
- 提供网络测试工具，如 Tracert、Ping 等，迅速诊断网络可达性；
- 提供种类丰富、内容详尽的调试信息，帮助诊断网络故障；
- 命令行解释器对关键字采取不完全匹配的搜索方法，用户只需键入无冲突关键字即可被解释，如命令 **display**，键入 **dis** 即可。

2. 命令行接口

防火墙的命令行接口提供了丰富的配置命令，在系统视图下全部命令被分组，每组对应一个视图，可以用命令在不同的视图之间切换。一般情况下，在某个视图下只能执行限定的命令，但对一些常用命令（如 **ping**、**display current-configuration**、**interface** 等）在各种视图下均可执行。

第5章 防火墙的软件维护

防火墙管理的文件包括三类：

- Boot ROM 程序文件
- 应用程序文件
- 配置文件

防火墙的软件维护主要是针对上面三类文件，包括：Boot ROM 程序文件、应用程序文件的升级下载及配置文件的上传下载等。

5.1 Boot 菜单

在防火墙的软件维护过程中需要使用 Boot 菜单，因此本节对 Boot 菜单进行介绍。

按照图 4-1所示搭建配置环境，然后启动防火墙，当配置终端上出现“Press Ctrl-B to enter Boot Menu”提示信息时，按下<Ctrl+B>键，系统将提示：

```
Please  input Boot ROM password :
```

⚠ 注意：

- 必须在出现“Press Ctrl-B to Enter Boot Menu...”的 3 秒钟之内，按下<Ctrl+B>键，才能进入 Boot 菜单，否则将进入程序解压过程。
- 若您在进入程序解压过程后希望进入 Boot 菜单，需要重新启动防火墙。

输入正确的口令后，键入<Enter>（如没有设置 Boot ROM 口令，直接键入<Enter>即可）系统将进入 Boot 菜单，显示如下：

1. H3C SecPath F100-A 防火墙的 Boot 菜单

```
Boot Menu:
     1:  Download application program with XMODEM
     2:  Download application program with NET
     3:  Display file in flash
     4:  Delete file from flash
     5:  Start up and ignore configuration
     6:  Enter debugging environment
     7:  Boot Rom Operation Menu
     8:  Do not check the version of the software
     9:  Exit and reboot
Enter your choice(1-9):
```

Boot 菜单各选项含义如下：

- 1：通过XModem下载应用程序，具体升级步骤请参见5.2 ；
- 2：通过以太网下载应用程序，H3C SecPath F100-A防火墙仅提供通过TFTP升级应用程序的方法，具体升级步骤请参见5.4 ；
- 3：显示 flash 中的文件；
- 4：从 flash 中删除文件；
- 5：忽略配置文件并以缺省配置启动；
- 6：进入调试环境；
- 7：进入 Boot ROM 操作子菜单；
- 8：不检查 Boot ROM 程序扩展段、Boot ROM 程序和应用程序的软件版本，此项用于版本升级时的后向兼容。当升级软件时，如采用的软件版本完全正确，仍无法升级成功，系统提示软件为“invalid version”，此时可选中此项，以便在软件升级时取消版本检查。此项被选中时只起作用一次，重新启动防火墙后即恢复版本检查；
- 9：退出 Boot 菜单并重新启动防火墙。

2. H3C SecPath F100-A 防火墙的 Boot ROM 子菜单

如前所述，进入 Boot 菜单后选择第 7 项即可进入 Boot ROM 子菜单，其内容如下：

```
Boot ROM Operation Menu:
     1:  Download Boot ROM with XModem
     2:  Download Extended Segment of Boot ROM with XModem
     3:  Restore Extended Segment of Boot ROM from FLASH
     4:  Backup Extended Segment of Boot ROM to FLASH
     5:  Exit to Main Menu
     Enter your choice(1-5):
```

各项含义如下：

- 1：通过 XModem 升级 Boot ROM 程序；
- 2：通过 XModem 升级 Boot ROM 程序扩展段；
- 3：从 FLASH 中恢复 Boot ROM 程序扩展段；
- 4：备份 Boot ROM 程序扩展段到 FLASH 中；
- 5：退回到主菜单。

该菜单中提供了Boot ROM程序升级、备份、恢复等方法，具体操作请参见5.2 、5.3 。

⚠ 注意：

请勿轻易进行防火墙的软件升级，最好在技术支持人员的指导下进行。另外在进行防火墙升级时，请注意 Boot ROM 软件和应用程序的版本匹配。

5.2 利用 XModem 协议完成应用程序和 Boot ROM 程序升级

利用 XModem 协议完成软件升级时直接使用配置口，不必另外搭建配置环境。

1. 应用程序的升级

第一步：进入Boot菜单（参见5.1 小节），键入<1>，选择通过XModem协议下载应用程序。防火墙将提供如下可供选择的下载速率：

```
Downloading application program from serial ...
Please choose your download speed:
1: 9600 bps
2: 19200 bps
3: 38400 bps
4: 57600 bps
5: 115200 bps
6: Exit to Main Menu
Enter your choice(1-6):
```

第二步：选择合适的下载速率，如键入<5>，选择 115200 bps 的下载速率，防火墙将提示如下信息：

```
Download speed is 115200 bps. Change the terminal's speed to 115200 bps, and
select XModem protocol. Press ENTER key when ready.
```

第三步：根据上面提示，改变配置终端设置的波特率（参考图 4-4），使其与所选的软件下载波特率一致。设置完终端波特率后，应做一次终端的断开（即[拨入/断开]）和拨号（即[拨入/拨号]）操作，然后按<Enter>键即可开始下载，系统提示如下：

```
Downloading ... CCCCC
```

🕮 说明：

设置完配置终端的波特率后，只有做一次终端仿真程序的断开和连接操作，新的设置才会有效。

第四步：从终端窗口选择[传送/发送文件]，弹出如下图所示的对话框：

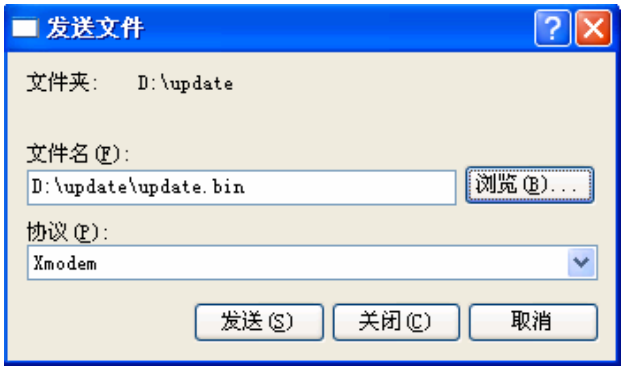


图5-1 [发送文件]对话框

第五步：点击[浏览]按钮，选择需要下载的应用程序文件，并将协议设置为 XModem，然后点击[发送]按钮，系统弹出如下界面：

图5-2 正在发送文件界面

第六步：下载完成后，系统开始写 Flash（闪速存储器）操作，当这一操作完成后，终端界面出现如下信息，表明下载完成：

```
XModem download completed, Packet length 8790321 bytes.
    System file length 7868992 bytes, http.zip file length 921329 bytes.

    Writing file flash:/system to FLASH...
    Please wait, it may take a long time
##################################################
    Writing into Flash Succeeds.

    Writing file flash:/http.zip to FLASH...
    Please wait, it may take a long time
##########################################################################
######
#########
```

```
    Writing into Flash Succeeds.
Please use 9600 bps.Press <ENTER> key to reboot the system.
```

此时按提示将配置终端速率恢复为 9600bps（并进行一次断开和拨号操作），然后系统正常启动。

2. Boot ROM 程序的升级

第一步：进入Boot菜单（参见5.1 小节），选择<7>，进入Boot ROM操作子菜单；

第二步：在Boot ROM操作子菜单中选择<1>，通过XModem升级Boot ROM程序，防火墙将提供多种可选择的速率，随后操作与5.2 中的“1. 应用程序的升级”中的描述相同。

⚠ 注意：

如果整个 Boot ROM 程序升级失败，将无法现场恢复，故只有在必要且有技术支持人员协助的情况下方可升级整个 Boot ROM 程序。

3. Boot ROM 程序扩展段的升级

第一步：进入Boot菜单（参见5.1 小节），选择<7>，进入Boot ROM操作子菜单；

第二步：在Boot ROM操作子菜单中选择<2>，通过XModem升级Boot ROM程序扩展段，防火墙将提供多种可选择的速率，随后操作与5.2 中的“1. 应用程序的升级”中的描述相同。

⚠ 注意：

采用这种方法升级 Boot ROM 程序只是升级了程序的一部分，一旦出现错误可以重新升级。

5.3 Boot ROM 程序扩展段的备份及恢复

1. 在 FLASH 中备份 Boot ROM 程序的扩展段

如果防火墙需要备份 Boot ROM 程序的扩展段，可以采用如下方法：

第一步：进入Boot菜单（操作方法见5.1 ），选择<7>，进入Boot ROM操作子菜单；

第二步：在 Boot ROM 操作子菜单中选择<4>，这样当前的 Boot ROM 程序扩展段将被复制到 FLASH 中。

```
Backup Extended Segment, are you sure?[Y/N]
```

键入<Y>，则开始备份；

如果备份成功，则提示信息如下：

```
Writing to FLASH.Please wait...####
Backuping Boot ROM program to FLASH successed!
```

第三步：当再次出现 Boot 子菜单时，选择<5>，退出并重启防火墙即可。

2. 从 FLASH 中恢复 Boot ROM 程序扩展段

在 Boot ROM 程序扩展段出现问题或被误升级的情况下，可以将以前在 FLASH 中备份的 Boot ROM 程序扩展段重新恢复到 Boot ROM 中，方法如下：

第一步：进入 Boot 菜单，选择<7>，进入 Boot ROM 操作子菜单（菜单内容如上所示）；

第二步：在 Boot ROM 操作子菜单中选择<3>，从 FLASH 中恢复 Boot ROM 程序扩展段，会出现如下提示：

```
Restore Extended Segment, are you sure?[Y/N]
```

键入<Y>，则开始恢复；

如果成功恢复，则出现如下提示：

```
Writing to Boot ROM.Please wait...######
Restoring Boot ROM program successed!
```

第三步：当再次出现 Boot 子菜单时，选择<5>，退出并重启防火墙即可。

5.4 通过 TFTP 完成应用程序的升级

通过网络下载应用程序是指通过以太网口下载应用程序，此时防火墙作为 Client ，需要在防火墙的固定以太网口上连接 TFTP Server。具体的升级方法如下：

⚠ 注意：

TFTP Server 程序由用户自己购买、安装，H3C SecPath F100-A 防火墙不提供此软件。

H3C SecPath F100-A 仅提供 TFTP client 的功能，故仅提供通过 TFTP 升级应用程序的方法，升级步骤如下：

(1) 启动 TFTP Server

在防火墙的以太网口所连接的 PC 上启动 TFTP Server，并设置好欲加载文件的所在路径。

(2) 配置防火墙

第一步：进入 TFTP 配置状态；

启动防火墙，进入Boot菜单（操作方法见5.1 ），选择<2>，进入Net Port Download Menu(网络下载菜单)；

显示如下：

```
Net Port Download Menu:
     1:  Change Net Parameter
     2:  Download From Net
     3:  Exit to Main Menu
     Enter your choice(1-3): 1
```

第二步：配置 TFTP 参数；

选择<1>，可配置防火墙的网络接口参数，包括防火墙使用的接口、接口 IP 地址、子网掩码等；以及 TFTP Server 参数，包括 TFTP Server 的以太网口 IP 地址、应用程序的文件名等。

```
    Change Download parameter
     Download device             :WAN2              下载所使用的设备名
     Download file(Max 60 char)  :system            服务器上的应用程序文件名
     IP address of WAN2          :192.168.1.15      防火墙接口的 IP 地址
     Subnet mask for WAN2        :255.255.255.0     防火墙接口的子网掩码
     IP address of the server    :192.168.1.10      TFTP 服务器的 IP 地址
     IP address of the gateway   :10.110.95.117     网关的 IP 地址
```

⚠ 注意：

- 必须使用防火墙的 WAN2 接口进行升级。
- “IP address of the server : [192.168.1.10]”一项必须设为防火墙以太网口所连的 TFTP Server 的 IP 地址。
- 建议将 TFTP Server 的网口 IP 地址与防火墙 WAN2 接口的 IP 地址设置为同一网段。

第三步：确认配置参数；

键入最后一项值后，将会出现如下提示并返回 Net Port Download Menu 菜单：

```
    Saving config, please wait...OK!
    Net Port Download Menu:
     1:  Change Net Parameter
     2:  Download From Net
     3:  Exit to Main Menu
     Enter your choice(1-3): 2
```

(3) 通过 TFTP 下载应用程序

按下<2>键，进入 TFTP 下载状态，提示如下：

```
Starting the TFTP download...
```

```
.....................................................................
.....................
    TFTP download completed, Packet length 8790321 bytes.
    System file length 7868992 bytes, http.zip file length 921329 bytes.

    Writing file flash:/system to FLASH...
    Please wait, it may take a long time
#########################################################################
Writing into Flash Succeeds.

    Writing file flash:/http.zip to FLASH...
    Please wait, it may take a long time
#########################################################################
######
#########
    Writing into Flash Succeeds.
```

加载成功，键入<Enter>后，系统正常启动。

5.5 利用 FTP 完成程序/文件的上传下载

H3C SecPath F100-A 防火墙提供 FTP Server 功能，为用户提供了另外一种更新配置文件、升级应用程序及 Boot ROM 程序的途径。任何 FTP Client（包括本地用户和远端用户）只要与防火墙连通即可。当通过用户验证后，即可进行配置文件或应用程序的上传下载。利用 FTP 上传/下载应用程序、配置文件及上传 Boot ROM 程序操作步骤如下：

📖 **说明：**

上传：从 FTP 客户端的微机向防火墙传送文件，即 put 操作。

下载：从防火墙向 FTP 客户端的微机传送文件，即 get 操作。

---

1. 搭建上传/下载环境

- 搭建 FTP 本地上传/下载环境

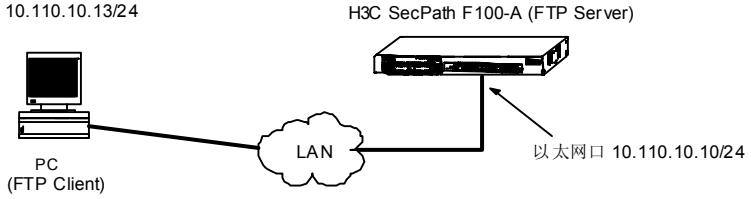


图5-3 搭建 FTP 本地上传/下载环境

第一步：通过防火墙以太网口连接微机；

第二步：配置防火墙以太网口 IP 地址，假设为 10.110.10.10；

第三步：配置微机以太网口 IP 地址，假设为 10.110.10.13；

第四步：将应用程序/Boot ROM 程序/配置文件等拷贝到某一路径下，假设路径为 C:\ version。

⚠ 注意：

微机网口 IP 地址与防火墙以太网口 IP 地址应位于同一网段。

- 搭建 FTP 远程上传/下载环境

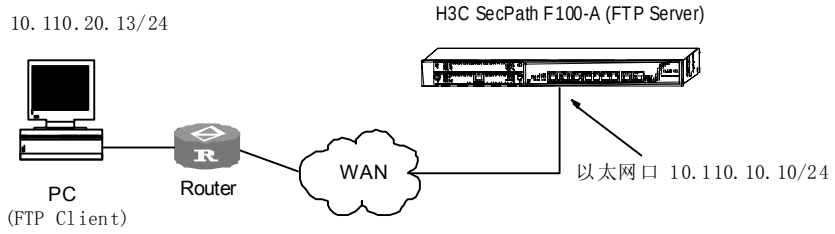


图5-4 搭建 FTP 远程上传/下载环境

第一步：将微机通过 WAN 连接至防火墙任意接口。这种方法不要求微机与防火墙在同一网段，用于防火墙远程升级；

第二步：将应用程序、Boot ROM 程序或配置文件拷贝到某一路径下，假设路径为 C:\version。

2. 启动 FTP 服务器

请防火墙侧维护人员进行配合，作如下配置：

第一步：设置验证方式；

📖 说明：

AAA 验证的具体配置您可以根据自己的实际情况进行选择，命令的详细介绍请参见本产品操作手册和命令手册的 AAA 和 RADIUS 配置。

第二步：添加用户名；

```
[VPNGateway] local-user VPNGateway
```

VPNGateway 表示用户名。

第三步：添加口令；

```
[VPNGateway-luser-vpngateway] password simple 123
```

第四步：添加服务类型，指定 FTP 目录；

```
[VPNGateway-luser-vpngateway] service-type ftp ftp-directory flash:
```

第五步：添加权限等级；

```
[VPNGateway-luser-vpngateway] level 3
```

第六步：启动 FTP 服务器。

```
[VPNGateway] ftp server enable
```

经过以上操作，在防火墙上已经启动了 FTP 服务器，并设置了用户，这样任何一个 FTP 客户端程序均可使用该用户名、口令登录 FTP 服务器。

3. 上传/下载应用程序、配置文件及上传 Boot ROM 程序

第一步：在 DOS 下进入应用程序、Boot ROM 程序或配置文件所在路径，然后执行 FTP 命令，与防火墙建立 FTP 连接，如：

```
C:\version\ftp 10.110.10.10
```

若连接成功，则显示（以 Windows98 为例）：

```
Connected to 10.110.10.10
220 FTP server ready on SecPath Gateway at
User(10.110.10.10:(none)):
```

第二步：使用已经在防火墙上设置好的用户名、口令登录 FTP 服务器；

```
User(10.110.10.10:(none)): SecPath Gateway                键入用户名
331 Password required for ftp
Password:                          键入口令（屏幕上不显示用户输入的口令）
230 User ftp logged in
ftp>
```

当出现提示符 ftp>时，表示可以进行上传下载操作了。

第三步：上传/下载应用程序、配置文件或上传 Boot ROM 程序；

📖 **说明：**

防火墙端应用程序缺省名称为 system，配置文件缺省名称为 config.cfg，Boot ROM 扩展段文件缺省名称为 bootrom，整个 Boot ROM 文件缺省名称为 bootromfull。

- 上传应用程序/Boot ROM 程序/配置文件

```
ftp> put          键入<put>，表示进行上传操作。
local file        键入要上传的应用程序/Boot ROM 程序/配置文件的名称。
remote file       键入防火墙端上传后所要保存的应用程序/Boot ROM 程序/配置文件名称。
```

上传文件结束后，重新显示“ftp>”提示符，可键入<dir>显示防火墙上的文件名称和大小，上传成功则配置文件大小与主机上的文件大小一致。

⚠ 注意：

- 当使用 **FTP** 对应用程序进行升级时，请确保防火墙的 Flash 中有足够的空间。若剩余空间不足，需使用 **delete /unreserved** 命令将旧版本或其他文件永久删除，否则无法上传新文件。
- 当使用 **put** 命令完成 Boot ROM 程序的上传后，还应接着使用 **upgrade bootrom** [**full**]命令将 bootrom/bootromfull 程序从 Flash 的根目录中解出，写到 Boot ROM 中，才能完成 Boot ROM 的升级。
- 将应用程序文件上传到 Flash 中后，若要使应用程序在下次启动时生效，需将文件重命名为 system。
- 将配置文件上传到 Flash 中后，若要使配置文件在下次启动时生效，需将文件重命名为 config.cfg，或使用 **startup saved-configuration** 命令设置系统下次启动时使用的配置文件。

- 下载应用程序/配置文件

ftp> get	键入<get>，表示进行下载操作。
remote file	键入防火墙端应用程序/配置文件名称。
local file	键入要保存的应用程序/配置文件的名称。

第四步：上传/下载成功后，退出 FTP 客户端程序。

ftp>quit	键入<quit>，表示退出 ftp 连接。

4. 使用 detach 命令将 Web 文件解包分离出来。

FTP 方式下载完成应用程序/配置文件后。当应用程序中包含 Web 文件时，还需使用 **detach** 命令将其解包分离出来才能使用。

```
<VPNGateway> detach system
    System file length 7856557 bytes, http file length 834724 bytes.
<VPNGateway> dir
Directory of flash:/
   0   -rw-   8691281  Jun 16 2009 06:46:36   system
   1   -rw-      1830  Jun 17 2009 07:47:16   config.cfg
   2   -rw-    834724  Jun 18 2009 02:22:39   http.zip
```

如果要解包的文件没有捆绑 Web 文件，则提示文件中没有捆绑 Web 文件；如果没有指定解包出的 Web 文件名，则 Web 文件名缺省为 http.zip。

5.6 修改 Boot ROM 口令

可以使用防火墙的 Boot 菜单更改 Boot ROM 的口令。

启动防火墙，当配置终端上出现“System starts booting”提示信息时，按下<Ctrl+D>键，系统将提示：

```
Please input Boot ROM password :
```

⚠ 注意：

- 必须在出现“System starts booting”的 3 秒钟之内，按下<Ctrl+D>键，才能进入 Boot 菜单，否则将进入程序解压过程。
- 若您在进入 Boot ROM 扩展段后希望进入 Loader 段菜单，需要重新启动防火墙。

输入正确的口令后，键入<Enter>（如果没有设置 Boot ROM 口令，直接键入<Enter>即可）系统将进入 Boot 菜单，显示信息如下：

```
Boot Menu:
   1:  Download Boot ROM with XModem
   2:  Download Extended Segment of Boot ROM with XModem
   3:  Modify Boot ROM password
   4:  System booting from Flash
   5:  Do not check the version of Extended Segment of Boot ROM
   6:  Exit and reboot
   Enter your choice(1-6):
```

Boot 菜单各选项含义如下：

- 1：通过 XModem 下载 Boot ROM 程序；
- 2：通过 XModem 升级 Boot ROM 程序扩展段；
- 3：修改 Boot ROM 密码；
- 4：从flash中引导Boot ROM扩展段；（此项功能需要flash中存在Boot ROM扩展段的备份，请参见5.3 。）；
- 5：不检查 Boot ROM 程序扩展段、Boot ROM 程序的软件版本；（此项功能用于版本升级时的后向兼容。当升级软件时，如采用的软件版本完全正确，仍无法升级成功，系统提示软件为“invalid version”，此时可选中此项，以便在软件升级时取消版本检查。此项被选中时只起作用一次，重新启动防火墙后即恢复版本检查）；
- 6：退出 Loader 段菜单并重新启动防火墙。

在 Boot 菜单中选择<3>，修改 Boot ROM 密码，提示信息如下：

```
Modify Boot ROM password, are you sure?[Y/N]y

Please input new password(Max 32 char) :
Retype  the  new password(Max 32 char) :
Saving the password... Success!
```

📖 **说明：**

密码的最大长度是 32 个字符。

5.7 口令丢失的处理

如果防火墙 Boot ROM 的口令或用户口令丢失，请与技术支持人员联系，技术支持人员会帮助您进入防火墙，并重新设置口令。

第6章 安装故障处理

6.1 电源系统问题故障处理

(1) 故障现象

电源指示灯 PWR 不亮。

(2) 故障处理

请进行如下检查：

- 防火墙电源开关是否打开。
- 防火墙供电电源开关是否打开。
- 防火墙电源线是否连接正确。
- 防火墙供电电源与防火墙所要求的电源是否匹配。

⚠ 注意：

请不要带电插拔电源线。如完成上述的检查工作后，电源指示灯 PWR 仍未变亮，请与代理商联系。

6.2 配置系统故障处理

防火墙上电后，如果系统正常，将在配置终端上显示启动信息；如果配置系统出现故障，配置终端可能无显示或者显示乱码。

1. 终端无显示故障处理

(1) 故障现象

防火墙上电后，配置终端无显示信息。

(2) 故障处理

第一步：首先要做以下检查：

- 电源系统是否正常。
- 配置口（Console）电缆是否正确连接。

第二步：如果以上检查未发现问题，很可能是配置电缆的问题或者终端（如超级终端）参数的设置错误，请进行相应的检查。

2. 终端显示乱码故障处理

(1) 故障现象

防火墙上电启动后，配置终端上显示乱码。

(2) 故障处理

请确认终端（如超级终端）的参数设置：波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无，终端仿真为 VT100。如参数设置与上不符，请重新配置。

6.3 应用软件升级故障处理

1. 故障 1

(1) 故障现象

启动防火墙，用 TFTP 方式升级 Comware 软件，结果显示如下：

```
Net Port Download Menu:
     1:  Change Net Parameter
     2:  Download From Net
     3:  Exit to Main Menu
     Enter your choice(1-3): 2

    Starting the TFTP download...

    Failed to connect the tftp server!!
    Please check the  network setting!!
```

(2) 故障处理

以上故障的产生是由于 TFTP Server 程序没打开或以太网连接出现故障(包括 IP 地址设置不正确、网线没插好等)，从而造成无法连接 TFTP Server。请打开 TFTP Server 程序并确定 IP 地址等参数设置正确且网线已经插好。

2. 故障 2

(1) 故障现象

启动防火墙，用 TFTP 方式升级 Comware 软件，结果显示如下：

```
Net Port Download Menu:
     1:  Change Net Parameter
     2:  Download From Net
     3:  Exit to Main Menu
     Enter your choice(1-3): 2
```

```
    Starting the TFTP download...

    Failed to find the updated file
    Please check the  network setting!!
```

(2) 故障处理

以上故障的产生是由于所下载的文件不存在或文件路径设置不正确，请确定所需要下载的文件位于 TFTP Server 所指定的目录。

3. 故障 3

(1) 故障现象

启动防火墙，用 TFTP 方式升级 Comware 软件，结果显示如下：

```
Net Port Download Menu:
     1:  Change Net Parameter
     2:  Download From Net
     3:  Exit to Main Menu
     Enter your choice(1-3): 2

    Starting the TFTP download...

    The downloaded software is not a valid version.
    Please download the correct version.
```

(2) 故障处理

以上故障的产生是由于下载的程序版本有误，无法通过版本检测。请确定应用程序版本正确无误。

📖 **说明：**

防火墙主机及智能接口卡上均贴有包含相关生产维修信息的条形码，如用户需要返修设备，请将故障设备的条形码反馈给代理商。

第7章 MIM 多功能接口模块

7.1 MIM 多功能接口模块的种类

H3C SecPath F100-A 防火墙支持多种多功能接口模块（MIM），H3C SecPath F100-A 防火墙可支持的类型如下：

- 1 端口 10Base-T/100Base-TX 快速以太网接口模块（1FE）
- 2 端口 10Base-T/100Base-TX 快速以太网接口模块（2FE）
- 4 端口 10Base-T/100Base-TX 快速以太网接口模块（4FE）
- 网络数据加密模块（HNDE）

7.2 MIM 多功能接口模块的安装与拆卸

注意：

MIM 多功能接口模块拉手条上的簧片对防火墙整机的电磁屏蔽有特殊的效果，用户在拆换接口模块的过程中，请保证簧片的完整，切不可将簧片去掉。

进行接口模块安装时，请仔细阅读《第 2 章 安装前的准备工作》。

1. 安装工具

- 防静电手腕

2. MIM 接口模块的安装

警告：

进行以下任何操作之前，请一定要确认已经关闭与防火墙相连的所有电源，否则可能导致操作人员触电或设备的损坏。

第一步：将防火墙的前面板面对操作者。

第二步：关掉电源并拔掉电源线。

第三步：选择标记有 SLOT 的插槽并将接口模块向防火墙内部推进，直到与防火墙前面板紧密接触为止。

第四步：拧紧松不脱螺钉，将接口模块固定在防火墙上。

第五步：打开防火墙电源开关，并检查防火墙上的 ACT 指示灯是否正常闪烁 ，灯闪烁表示接口模块已经正确安装。

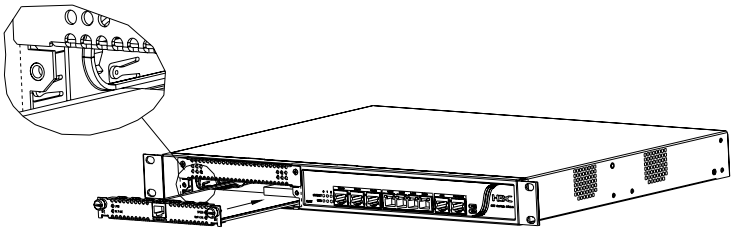


图7-1 MIM 多功能接口模块安装示意图 1

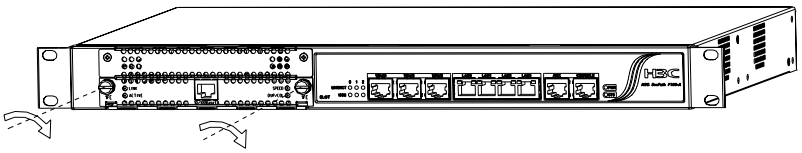


图7-2 MIM 多功能接口模块安装示意图 2

3. MIM 接口模块的拆卸

第一步：将防火墙的前面板面对操作者。

第二步：关掉电源并拔掉电源线。

第三步：拔掉防火墙前面板上所有接口模块的接口电缆。

第四步：松开接口模块两侧的松不脱螺钉。

第五步：将接口模块向操作者身前方向拖动，直到完全脱离防火墙底座为止。

⚠ 注意：

拆卸 MIM 接口模块时，应注意如下事项：

- 若 MIM 接口模块拆卸完成后无须安装新的接口模块，请及时安装空挡板，以防止灰尘进入，并保证防火墙的正常通风；
- 拆卸 MIM 接口模块时，请与工作间的过道保持一定距离，防止过往人员碰掉拆卸的模块或在拆卸过程中由于碰撞导致事故。

7.3 MIM 接口模块的故障处理

H3C SecPath 系列防火墙的 MIM 接口模块面板为用户提供有指示灯，用户可以根据指示灯的状态来判断接口模块安装是否正确。

若防火墙的接口模块出现工作异常，可按照如下方法来检查：

- 检查接口电缆，判断电缆是否选配正确。

- 观察各接口模块指示灯，判断接口模块工作是否正常。
- 根据配置中的 **display** 命令显示，判断接口是否接受配置，正常工作。

7.4 1FE/2FE/4FE 接口模块

7.4.1 简介

1FE/2FE/4FE 是 1/2/4 端口 10Base-T/100Base-TX 快速以太网接口模块的简称，其中 FE（Fast Ethernet）是快速以太网的英文缩写。FE 接口模块主要用于完成防火墙与局域网的通信。

防火墙包含三种型号的 FE 接口模块：1FE、2FE、4FE。

1FE、2FE、4FE 模块的区别在于：

- 1FE 接口模块提供 1 个 10/100Mbps 以太网 RJ45 接口。
- 2FE 接口模块提供 2 个 10/100Mbps 以太网 RJ45 接口。
- 4FE 接口模块提供 4 个 10/100Mbps 以太网 RJ45 接口。

FE 接口模块支持功能如下：

- 当用户采用 5 类双绞线时，可支持 100 米的传输距离。
- 接口可以工作在 100Mbps、10Mbps 两种速率下，且能实现自适应。
- 接口有全双工和半双工两种工作方式，且全双工是比较常用的工作方式。

7.4.2 接口模块外观

1. 1FE 接口模块外观

1FE 接口模块外观如下图所示：

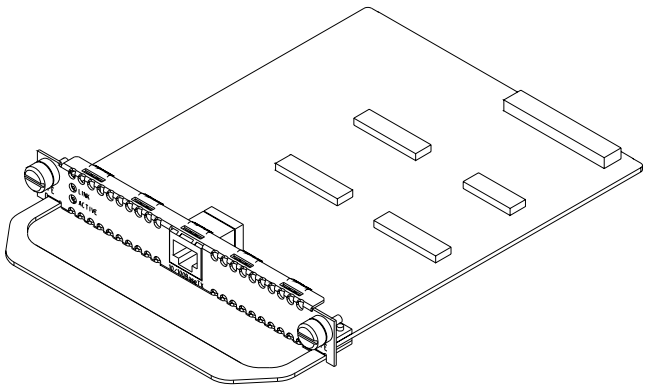


图7-3 1FE 接口模块外观

2. 2FE 接口模块外观

2FE 接口模块外观如下图所示：

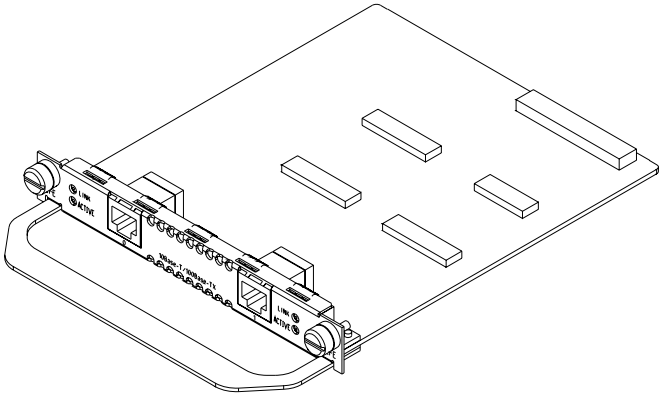


图7-4 2FE 接口模块外观

3. 4FE 接口模块外观

4FE 接口模块外观如下图所示：

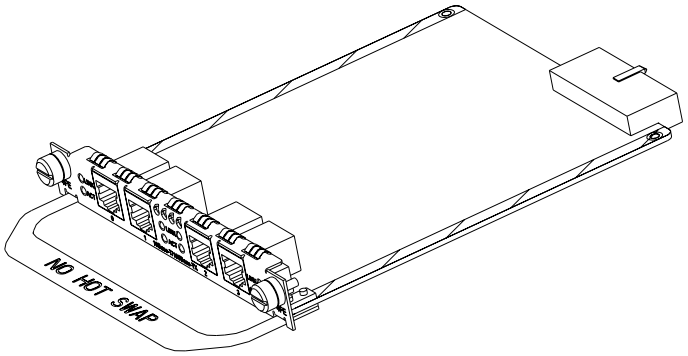


图7-5 4FE 接口模块外观

7.4.3 接口属性

1FE、2FE、4FE 接口属性如下表所示：

表7-1 1FE/2FE/4FE 模块接口属性

属性	描述		
	1FE 模块	2FE 模块	4FE 模块
连接器类型	RJ45		
连接器数量	1	2	4
电缆类型	标准以太网线		
工作方式	全双工/半双工 10M/100Mbps 自适应		
支持帧格式	Ethernet_II Ethernet_SNAP		

7.4.4 面板及接口指示灯

1FE 接口模块的面板如下图所示：

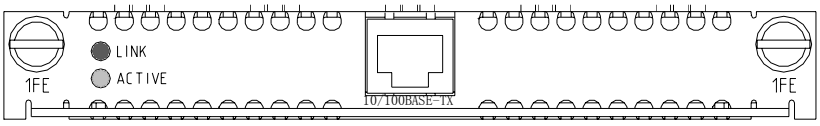


图7-6 1FE 接口模块面板

2FE 接口模块的面板如下图所示：

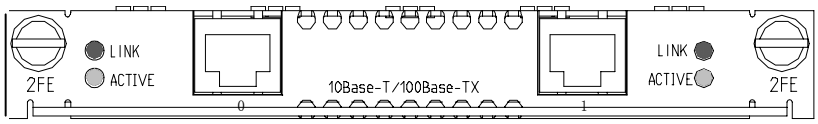


图7-7 2FE 接口模块面板

4FE 接口模块的面板如下图所示：

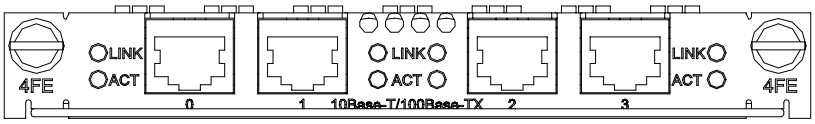


图7-8 4FE 接口模块面板

1FE/2FE/4FE 接口模块面板上的指示灯含义如下：

表7-2 1FE/2FE/4FE 接口模块指示灯含义

指示灯	含义
LINK	灯灭表示链路没有连通，灯亮表示链路已经连通。
ACTIVE	灯灭表示没有数据收发，灯闪烁表示有数据收发。

7.4.5 接口连接电缆

1. 以太网电缆外观

FE 接口电缆为带 RJ45 接头（参见下图）的 5 类双绞线电缆，其接口的 1、2 管脚为发送端，3、6 管脚为接收端。

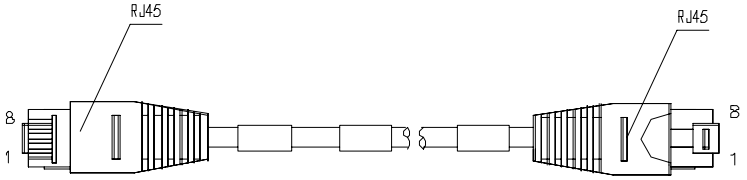


图7-9 以太网电缆

2. 以太网电缆的制作

下图为采用 5 类双绞线制作 RJ45 接头的以太网线缆示例，供用户使用时参考。5 类双绞线有 8 芯细线组成，利用细线外绝缘层上的颜色进行分组标识。通常利用单色和单色加上白色作为成对标识，也有利用色点成对进行标识的，本示例采用前者。

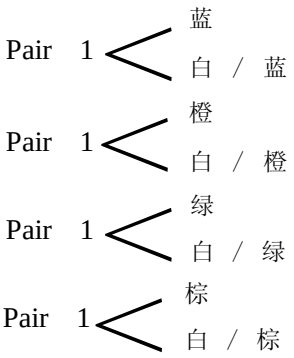


图7-10 5 类双绞线示例图

表7-3 标准（直通）网线连接关系表

RJ45	信号	5 类双绞线	信号方向	RJ45
1	TX+	白（橙）	→	1
2	TX-	橙	→	2
3	RX+	白（绿）	←	3
4	-	蓝	-	4
5	-	白（蓝）	-	5
6	RX-	绿	←	6
7	-	白（棕）	-	7
8	-	棕	-	8

表7-4 交叉网线连接关系表

RJ45	信号方向	5 类双绞线	信号方向	RJ45
1	TX+	白（橙）	→	3
2	TX-	橙	→	6
3	RX+	白（绿）	←	1
4	-	蓝	-	4
5	-	白（蓝）	-	5
6	RX-	绿	←	2
7	-	白（棕）	-	7

RJ45	信号方向	5 类双绞线	信号方向	RJ45
8	-	棕	-	8

因使用情况不同又可将以太网线分为标准网线（即直通网线）和交叉网线两种，分别介绍如下：

- 标准网线：又称直通网线，两端 RJ45 接头压接的双绞线的线序完全相同，用于终端设备（如 PC、路由器等）到 HUB 或 LAN Switch 的连接。
- 交叉网线：两端 RJ45 接头压接的双绞线的线序不相同，用于终端设备（如 PC、路由器等）到终端设备（如 PC、路由器等）的连接。用户需要可以自行制作。

📖 说明：

用户制作网线时，请优先采用屏蔽电缆，以保证电磁兼容的需要。

7.4.6 接口电缆的连接

第一步：如果需要连接防火墙到 PC 或路由器，请使用交叉网线，连接网线的一端到防火墙 FE 接口模块的以太网口，连接另一端到 PC 或路由器；如果需要连接防火墙到 HUB 或 LAN Switch，请使用标准网线，连接网线的一端到防火墙 FE 接口模块的以太网口，连接另一端到 HUB 或 LAN Switch。

第二步：上电后请检查 FE 接口模块面板上 LINK 指示灯的状态。LINK 灯亮表示链路已经连通，LINK 灯灭表示链路没有连通，请检查线路。

⚠ 注意：

连接时请认准接口上的标识，以免误插入其它接口，导致接口模块或防火墙主机的损坏。

7.5 HNDE 模块

7.5.1 模块简介

HNDE（High Network Data Encryption，高性能网络数据加密）支持 IPsec 协议，通过硬件加速 IP 数据包的加密处理，支持多种硬件加/解密和散列运算，提供了高性能、高可靠性的加密特性。

HNDE 可安装于部分 SecPath 系列安全产品的 MIM 插槽上，当插入 HNDE 模块时，设备主板完成 IP 包路由转发处理并实现含有加密特性的 VPN，由加密卡完成其中的加密工作。

7.5.2 模块属性

表7-5 HNDE 模块属性

属性	描述
支持的协议	IPsec
硬件实现算法	密钥算法 （DES、3DES、AES） 验证算法（HMAC-MD5-96，HMAC-SHA-1-96）

7.5.3 模块运行指示灯

高性能网络数据加密模块前面板如图所示：

图7-11 HNDE 模块面板

表7-6 HNDE 模块指示灯含义

指示灯	含义
STATUS	常亮（绿色）：表示模块上电正常 灭：表示模块没有加电，模块电源不工作或严重硬件故障
ACTIVE	闪烁（黄色）2 秒钟后灯灭：表示模块初始化完成 连续闪烁：表示模块正常运行，且与主机之间有数据收发 灭：表示模块正常运行，与主机之间无数据收发

7.5.4 模块故障排除

(1) 故障 1：开机后 STATUS 灯常灭。

排除：开机后 STATUS 灯应保持常亮。一直没有亮，说明模块或模块上的某些硬件没有正常加电。请您检查整机电源是否连接正确。

如果整机电源已经工作，可能模块的电源损坏，也可能 CPLD（Complex Programmable Logic Device）工作不正常，请与负责销售的代理商联系。

(2) 故障 2：开机过程中 ACTIVE 灯常灭。

排除：开机过程中，ACTIVE 灯应该闪烁 2 秒钟，然后熄灭，这表明模块的加密处理器已经配置完成，准备工作。如果在开机过程中 ACTIVE 灯保持常灭，即模块处理器初始化配置失败，说明可能是系统总线没有正常工作。请您检查模块是否和主机插接完好，如果插接完好，则可能是主机或模块存在问题，请与负责销售的代理商联系。

(3) 故障 3：模块运行中 ACTIVE 灯常亮或常灭。

排除：模块在运行加密业务时 ACTIVE 灯应闪烁，常亮或常灭说明可能是系统总线没有正常工作。请您检查模块是否和主机插接完好，如果插接完好，说明是主机或模块存在问题，请与负责销售的代理商联系。